monocone.com セキュリティチェックシート

■ 本チェックシートは、株式会社LIGHTzが提供する「ものづくりコネクト®クラウドサービス」について、セキュリティ対策に係わる情報を記載したものです。
■ 株式会社LIGHTzは、情報セキュリティマネジメントシステムについて ISO/IEC27001:2013/JIS Q 27001:2014 の要求事項に適合し、認証登録番号 JQA-IM1944 を保有しています。
■ 株式会社LIGHTzは、クラウドサービスセキュリティシステムについて ISO/IEC 27017 の要求事項に適合し、認証登録番号 JQA-IC0112 を保有しています。
■ 本チェックシートは、経済産業省が策定した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年度版」を基に、株式会社LIGHTzにて任意で項目の追加削除、及び主客体の解釈を加えて作成したものです。
(https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf)

項番	対策項目	対策要件	LIGHTz 実施内容
1．情報セキュリティへの組織的取組の基本方針			
組織の基本的な方針を定めた文書			
1	方針の作成・承認・配布	クラウドサービス事業者は、組織全体での情報セキュリティに関する取組についての基本的な方針、役割、責任等を定めた文書を作成し、経営陣の承認及び署名等を経て、組織内及び関係する組織に配布すること。	情報セキュリティマネジメントシステム(以下、「ISMS」)を構築し、情報セキュリティ保全活動を効果的に推進するために、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、体制の構築、監査及び見直しを行う仕組みを確立しております。
2	方針の変更	情報セキュリティに関する基本的な方針を定めた文書は、定期的又はクラウドサービスの提供に係る重大な変更や不適合が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。事業者は、経営陣の承認の下で方針の改定等を実施し、組織内及び関係する組織に通知すること。	ISMS運営事務局により、定期的な文書の見直し、セキュリティインシデント発生後の対策結果を盛り込む見直しを実施しております。改訂後は教育を含め組織に周知徹底を行っております。
2．情報セキュリティのための組織			
内部組織			
1	情報セキュリティ責任者	経営陣は、情報セキュリティに関する取組についての責任と関与を明示する。更に、組織全体にわたる情報セキュリティに責任を持つ情報セキュリティ責任者を任命し、人員・資産・予算等のリソース面で積極的な支援・支持を行うこと。	ISMSにより情報セキュリティに対する体制を策定し、ISMS事務局により適切に運営を行っています。
2	システム一覧	情報セキュリティ責任者は、組織が保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、全ての責任者を定めるとともに、個々の組織の職務記述書にセキュリティとプライバシーに関する役割と責任を記載すること。	使用するシステムについて一覧を作成、情報セキュリティ、ユーザー管理について役割、責任者、確認者を設置しています。また、定期的なリストの見直しを行っています。
3	テスト、トレーニング及び監視	組織全体にわたって実施されるセキュリティテスト、プライバシーテスト、トレーニングを監視すること。	ISMSにて情報セキュリティに関するトレーニング並びにテストを定期的に実施しております。
モバイル機器及びテレワーキング			
4	モバイル機器の利用方針	モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じること。	ISMSにてモバイルに関する利用方針を作成、並びにMDM(Mobile Device Management)による端末管理を実施しております。
5	テレワーキングでの情報保護	テレワーキングでアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施すること。	ISMSにて業務に関するアクセスネットワーク規定を設け、情報セキュリティの対策を行っています。
3．サプライチェーンに関する管理			
サプライチェーン事業者間の合意			
1	リスク対策と文書化	サプライチェーン事業者が提供するクラウドサービスについて、事業者間で合意された情報セキュリティリスク対策及びサービスレベルを文書化するとともに、サプライチェーン事業者によって確実に実施されることを担保すること。	弊社プロダクトは、Microsoftのクラウド環境を利用しております。クラウド事業者との責任分担については、以下のリンクをご確認ください。 https://learn.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility
4．情報資産の管理			
情報資産に対する責任			
1	管理責任者	取り扱う各情報資産について管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にした上で管理するとともに、文書化すること。	ISMSにより情報セキュリティに対する体制を策定し、ISMS事務局により適切に運営を行っています。
2	事業者間の引継ぎ	クラウドサービス利用者がクラウドサービスの利用を終了するにあたり、他のクラウドサービスへの乗換を行うことが想定される。クラウドサービス利用者によるクラウドサービス選定の自由を守るため、事業者は預託された情報を他のクラウドサービスに引き継ぐか否かに関して、予め利用者と合意し、文書化すること。	ひろめるプランにてデータのダウンロード機能がございます。ユーザー様ご自身でデータ移行を実施頂けます。ただし、ひろめるフリープランの場合はこの限りではありません。
3	バックアップ	情報、ソフトウェア及びシステムのバックアップは、利用者と合意されたバックアップ方針に従って、事業者が定期的に実施し、バックアップ内容を検査すること。また、事業者は、利用者にバックアップ機能の仕様を提供すること。	■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf RPOについては10分、RTOについては、1営業日にて設定しています。 ■文書ファイル ・継続的にバックアップを取得 ■データベース(文書ファイル以外のデータ) ・週毎 完全バックアップ ・12時間ごと 差分バックアップ ・10分ごと トランザクションログバックアップ
情報の分類			
4	資産目録	組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、機密性や重要性の観点から情報資産を分類した上で、資産目録を作成し、維持すること。	ISMSにて資産リストを作成、定期的な棚卸しチェックを実施しております。
5	データ識別	事業者は、利用者のデータ及びクラウドサービスから派生したデータを明確に識別すること。	弊社は、お客様データを閲覧しません。またクラウドサービスから派生するログについては別途区別されたストレージに保管し識別します。データや個人情報に関する規定については利用規約をご確認ください。 ■利用規約(第12条、第13条、第14条、第15条、第16条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf
6	情報資産の取扱い	情報資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施すること。	ISMSにて資産リストを作成、定期的な棚卸しチェックを実施しております。
情報セキュリティポリシーの遵守、点検及び監査			
7	レビュー	各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるように、定期的にレビュー及び見直しを行うこと。また、組織の情報セキュリティのための方針群及び標準に関し、システムや提供するクラウドサービスが、定めに従って技術的に順守されていることをレビューすること。	ISMSにより情報セキュリティに対する体制を策定し、ISMS事務局により適切に運営を行っています。またクラウドサービスの技術的な情報セキュリティ構成については、定期的なレビューを行い環境の保全を行っています。
8	点検・監査	クラウドサービスの提供に用いるシステムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に検証・監査すること。システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、実施すること。	ISMS審査員により、定期的に監査を実施しております。
アクセス管理			
9	アクセス制御方針	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューすること。また、情報及びシステム機能へのアクセスは、アクセス制御方針に従って、制限すること。	ISMSに則り、アクセス制御方式を制御しております。 また、サービス別のアクセス方式を文書化して管理しております。
10	アクセス制御	事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス及び利用者データへのアクセスを、利用者が制限できるようにアクセス制御を提供すること。	利用者はクラウドサービスの利用ができないよう権限整理を実施しています。 また、利用者は他テナントのデータを参照できないようにアクセス制御を実施しています。

11	ユーティリティプログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラム(データベースの中身を強制的に書き換えることが出来る機能や一時的にポートを開放する機能等)の使用は、制限し、厳しく管理すること。また、事業者は、クラウドサービス内で利用される全てのユーティリティプログラムのための要求事項を特定すること。	アプリケーションによる制御を無効にすることのできるプログラムはサービス管理者のみが利用できるよう制限しています。
12	プログラムソースコードへのアクセス	プログラムソースコードへのアクセスは、制限すること。	プログラムソースコードへのアクセスは必要な開発者のみに権限を付与しており、2FAを必須としています。
13	アクセス制御となりすまし対策	利用者及びシステム管理者等のアクセスを管理するために、適切な認証方法、特定の場所や装置からの接続を認証する方法等によって、アクセス制御となりすまし対策を行うこと。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法とパスワードの有効期限を規定に含めること。	利用者は、サインアップ時にメールアドレス認証を実施しています。 システム管理者と運用管理者はログインに多要素認証を設定することにより、なりすまし対策を行っています。
構成管理			
14	構成管理のポリシーと手順	目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンスを取り扱う構成管理ポリシー及び構成管理ポリシーと関連する対応策の実施手順を策定・文書化すること。	構成管理ポリシーはツールを用いて適用しています。
5．従業員に係る情報セキュリティ			
雇用前			
1	雇用契約	雇用予定の従業員(就業形態に関わらず)に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。	雇用前の従業員に対して、公開されている以上の機密性、完全性、可用性に関する開示は一切行いません。
雇用期間中			
2	教育・訓練	全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。	ISMSにて情報セキュリティに関するトレーニング並びにテストを定期的に実施しております。
3	契約違反	従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えること。	雇用契約ならびに就業規則にて規定を定め、懲戒の対象となることが規則に明記されております。
雇用の終了又は変更			
4	アクセス権・資産の取扱い	従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にすること。	情報システム部の手順ならびにチェックリストにより弊社システムからアカウントの凍結を行い情報資産へのアクセスを制限しています。
6．情報セキュリティインシデントの管理			
情報セキュリティインシデント及びぜい弱性の報告			
1	組織内報告	全ての従業員に対し、業務において発見あるいは疑いをもったシステムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施を要求すること。報告を受けた後に、迅速に効果的な対応ができるよう、責任体制及び手順を確立すること。	ISMSにより情報セキュリティに対する体制を策定し、ISMS事務局により適切に運営を行っています。情報セキュリティインシデントが発生した場合、同様に報告経路を定め適切に対応、管理を実施しています。
2	クラウドサービス事業者とクラウドサービス利用者間の報告	事業者は、利用者が情報セキュリティ事象を事業者に報告する仕組み、事業者が情報セキュリティ事象を利用者に報告する仕組み及び利用者が報告を受けた情報セキュリティ事象の状況を追跡する仕組みを提供すること。	事業者への報告につきましては、プロダクトホームページのお問い合わせより報告して頂く事が出来ます。 https://www.monocone.com また情報セキュリティインシデントが発生した場合の通知については、弊社システムにてリストメールにて報告させて頂きます。
3	インシデントの評価と分類	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定すること。	ISMS事務局に報告後、事象の評価を行い分類を行います。
4	フィードバック	情報セキュリティインシデントの分析及び解決から得られた知識は、情報セキュリティインシデントが将来起こる可能性又はその影響を低減するために用いること。	情報セキュリティインシデント対応後、対応結果の報告を行い、ISMS事務局にて再発防止策の提言を実施します。再発防止策については全社にて掲示を行います。
7．コンプライアンス			
法令と規則の遵守			
1	関連法規と記録	個人情報、要配慮個人情報、プライバシー情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。また、クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）について、法令、契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理するとともに、利用者から求められたときには提供すること。	利用規約に従って取り扱っております。 ■利用規約(第12条、第13条、第14条、第15条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf
2	利用可否	利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のためにシステム及び情報処理施設を利用させないこと。	使用するシステムについて一覧を作成、ユーザー管理について役割、責任者、確認者を設置しています。都度、ユーザーのメンテナンス、アクセス権の管理を実施しています。
3	ソフトウェア製品	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施すること。	弊社で利用するソフトウェア製品については、利用規約、契約書等を法務、ワークフローにて承認を得たものだけを利用しています。
4	不正アクセス・流出からの保護	記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護すること。また、事業者は、利用者によるクラウドサービスの利用に関連して、事業者が収集し、保存する記録の保護に関する情報を、利用者に提供すること。	利用規約に従って取り扱っております。 ■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf
5	暗号化	暗号化機能は、関連する全ての協定、法令及び規制を順守して用いるとともに、利用者が法令及び規制の順守をレビューできるようにするために、事業者は実施している暗号による対応策を記載すること。	当社ホームページのプライバシーポリシーにて定めております。 ■プライバシーポリシー https://lightz-inc.com/privacy-policy.html
8．ユーザサポートの責任			
利用者への責任			
1	SLA	事業者自身の責任範囲を SLA 等により文書化し、クラウド利用者に明確に示すこと。	責任範囲については、利用規約に記載をしております。 ■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf
保守			
1	システム保守ポリシーと手順	システム保守の目的、適用範囲、役割、責任、経営コミットメント、組織間の調整及び保守ポリシーを策定、文書化し、関係する組織に配布すること。	現状文書化したものはありません。 今後作成予定です。
2	保守ツール	システムの保守ツールを承認・管理し、モニタリングするとともに、以前の保守ツール使用状況レビューすること。	保守ツールの承認と管理を行っている。
3	リモート保守	リモート保守及び診断を承認のうえモニタリングする。リモート保守及び診断用ツールは、組織のポリシーに沿い、かつシステムのセキュリティ計画に記載されている通りである場合のみ、使用を許可すること。また、リモート保守及び診断のためのセッションを確立する際には、厳格な認証機能を使用するのに加え、リモート保守及び診断の記録を保管すること。リモート保守が完了したら、セッションとネットワーク接続を終了すること。	リモート保守での認証を実施しており、作業内容のログを保存しております。
4	保守要員	保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持すること。	保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を作成済みです。
5	タイムリーな保守	システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートを行うこと。	弊社営業日カレンダーに従い、平日9:00-18:00の間のみサポートを実施します。時間外での対応については、ベストエフォートにて対応を行います。 ■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf
9．事業継続マネジメントにおける情報セキュリティ			
緊急時対応計画			

2	緊急時対応計画の策定と手順	目的・適用範囲・役割・責任・経営コミットメント、組織間の調整及びコンプライアンスを取り扱う緊急時対応計画を策定するとともに、「緊急時対応計画」の実施手順を策定・文書化すること。	弊社営業日カレンダーに従い、平日9:00-18:00の間のみサポートを実施します。時間外での対応については、ベストエフォートにて対応を行います。 ■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf
１０．その他			
暗号と認証			
1	方針	情報を保護するための暗号利用に関する方針を、策定し、実施すること。	当社ホームページのプライバシーポリシーにて定めております。 ■プライバシーポリシー https://lightz-inc.com/privacy-policy.html
2	情報提供	事業者は、利用者に、事業者が処理する情報を保護するために、暗号を利用する環境に関する情報を提供すること。また、事業者は、利用者自らの暗号による保護を適用することを支援するために、事業者が提供する能力についても利用者に情報を提供すること。	当社ホームページのプライバシーポリシーにて定めております。 ■プライバシーポリシー https://lightz-inc.com/privacy-policy.html データの暗号化について、利用者が指定する暗号化方式を採用することや、利用者が独自に暗号化するなどの機能は提供をしていません。
3	暗号鍵の作成と管理	組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄すること。	弊社内ポリシーに則って管理しております。
１１．運用における情報セキュリティ			
運用管理			
1	情報セキュリティ監視手順の策定	情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。また、クラウドサービスの提供に用いるアプリケーションの運用・管理に関する手順書を作成すること。	監視基準及び手順書をまとめ、運用・管理を実施しております。
2	運用管理端末	運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全ファイルのウイルスチェックを行うこと。	運用端末には弊社から許可されたプログラムのみをインストールしています。またセキュリティソフトウェアにてウイルスチェック等のセキュリティ対策を常時行っています。
3	稼働・障害監視	クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行うこと。稼働停止や異常を検知した場合は、クラウドサービス利用者に速報すること。また、結果を評価・総括して、管理責任者に報告すること。	監視の仕組みを構築しているため、異常が発生した場合には、検知しております。 お客様への影響がある場合は、ご契約管理者様へメールを送付させて頂きます。
4	追加報告	クラウドサービスの提供に用いるアプリケーションに係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告をクラウドサービス利用者に対して行うこと。	上記同様、お客様への影響がある場合は、ご契約管理者様へメールを送付させて頂きます。
5	時刻同期	クラウドサービスの提供に用いるアプリケーションの時刻同期の方法を規定し、実施すること。	Microsoftのクラウド環境内にあるNTPサーバと時刻同期を実施しております。
6	パスワード管理	パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にすること。	パスワードについては、弊社ISMSの規程に従い適切に運用しております。また環境へのアクセスについては、パスワードの他、2FAを採用することによりセキュリティレベルを高めています。
7	クラウドサービスの変更管理	情報セキュリティに影響を与える組織、業務プロセス及びシステムの変更を管理すること。また、事業者は、クラウドサービスに影響を与える可能性のあるクラウドサービスの変更について、利用者に情報を提供すること。	情報セキュリティに関する組織、業務の変更については、弊社ホームページのプレスリリース、ならびにお知らせにて随時公開しております。 https://www.lightz-inc.com/ クラウドサービスに関する変更につきましては、随時ご契約管理者様へメールを送付させて頂きます。
8	リソース監視	要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測すること。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視すること。	資源の利用状況を監視しており、かつ定期的に見直しを行っております。
9	環境分離	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために分離すること。	開発環境と運用環境を分離しております。
10	マルウェア対策	マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。	開発者のPCにウイルス対策ソフトを入れて対策をしております。 サーバに関しては、アクセス元制限やIDベースの認証等により保護を実施しております。また、サーバはPaaS利用のため、OS領域に関してはクラウド事業者が対策をしております。 問題が生じた場合は、すぐにクラウドリソースを再構築することで対応できる状態にしてあります。
11	イベントログの取得	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューすること。また、事業者は、利用者に、ログ取得機能を提供すること。	利用者のログについてはイベントログを取得しております。ただしすべてのログのレビユーや利用者へのログ提供は実施しておりません。
12	ログの保護	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護すること。	ログの改竄ができないように制限をかけております。
13	技術的ぜい弱性	利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに獲得すること。また、そのようなぜい弱性に組織がさらされている状況を評価すること。さらに、それらと関連するリスクに対処するために、適切な手段をとること。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。	技術的脆弱性に関する情報は、ウィルス、スパイウエア、技術的脆弱性等への対策について、情報収集と情報周知を実施しております。
システム及び情報の完全性			
14	セキュリティ侵害の検知	システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたり、不適切に変更、削除されたりしたかを検知すること。	プログラムのソースコードが変更された場合、コミュニケーションツールに通知を送っております。 また、変更する際には開発者同士でのレビューが必須となっているため、悪意のある変更はなされません。
１２．アプリケーション			
アプリケーションの情報セキュリティ対策			
1	ウイルス対策	クラウドサービスの提供に用いるアプリケーション（データ・プログラム等）についてウイルス等に対する対策を講じること。	開発者のPCにウイルス対策ソフトを入れて対策をしております。 サーバに関しては、アクセス元制限やIDベースの認証等により保護を実施しております。また、サーバはPaaS利用のため、OS領域に関してはクラウド事業者が対策をしております。 問題が生じた場合は、すぐにクラウドリソースを再構築することで対応できる状態にしてあります。
2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護すること。	WAF(web application firewall)を導入することにより、サイバー攻撃からアプリケーションの保護を実施しております。
3	アプリケーションサービスのトランザクションの保護	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護すること。 ・不完全な通信 ・誤った通信経路設定 ・認可されていないメッセージの変更 ・認可されていない開示 ・認可されていないメッセージの複製又は再生	アプリケーションサービスの通信はHTTPS通信以外受け付けないよう設定しております。 また、WAF(web application firewall)を導入することにより、サイバー攻撃からアプリケーションの保護を実施しているため、認可されていないものは受け入れないような仕組みになっております。
4	プラットフォーム変更後のアプリケーションの技術的レビュー	プラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験すること。	アプリケーションの変更は開発者同士のレビューを必須としており、開発環境での試験を実施しております。試験において問題なかったアプリケーションのみを運用環境に適用しております。
データの保護			

5	バックアップ	利用者のデータ、アプリケーションの管理情報及びシステム構成情報の定期的なバックアップを実施すること。	■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf RPOについては10分、RTOについては、1営業日にて設定しています。 ■文書ファイル ・継続的にバックアップを取得 ■データベース(文書ファイル以外のデータ) ・週毎 完全バックアップ ・12時間ごと 差分バックアップ ・10分ごと トランザクションログバックアップ ■アプリケーション、システム構成情報については、ソースコードでの管理を行っております。
セッション管理			
6	セッションのライフサイクル管理	セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
7	セッションの真正性	通信セッションの真正性を保護すること。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
8	同時セッションの制御	同時処理されるアカウントの割り当て数、又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
9	セッションのロック	定められたアイドル時間を経過した場合、又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
13．プラットフォーム、サーバ・ストレージ			
プラットフォーム、サーバ・ストレージの情報セキュリティ対策			
1	ウイルス対策	クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージについてウイルス等に対する対策を講じること。	PaaSサービスをメインに利用しているため、プラットフォームはMicrosoftによりウイルス対策が講じられております。
プラットフォーム、サーバ・ストレージの運用・管理			
2	可用性	クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率を規定すること。また、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。	利用規約に従って取り扱っております。 ■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf
3	リソース	クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。	利用状況予測を文書化し、それを元にプラットフォームの性能を判断しております。
データの保護			
4	バックアップ	利用者のサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。	利用規約に従って取り扱っております。 ■利用規約(第11条) https://stpincypublicprod.z11.web.core.windows.net/monocone_userpolicy_r1.pdf 管理情報及びシステム構成情報は定期的なバックアップを実施しております。
14．ネットワーク			
ネットワークにおける情報セキュリティ対策			
1	ネットワーク構成	ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。	ネットワーク構成図を作成しております。 アクセス制御のための手順を策定して運用しております。
2	管理者の権限	情報セキュリティ責任者は、システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。	情報セキュリティ責任者が必要な権限の割当及び使用を制限しております。
3	不正アクセス防止	外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。	WAF(web application firewall)の導入とIP制限を実施しております。
5	実施基準	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。	通信をHTTPS通信のみに設定し、通信経路を保護しております。
6	通信の暗号化	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	通信をHTTPS通信のみに設定し、通信経路を保護しております。
7	サーバ証明書	第三者が当該事業者のサーバになりますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。	サーバ証明書を利用して、通信を暗号化しております。
セッション管理			
9	セッションのライフサイクル管理	セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
10	セッションの真正性	システムは、通信セッションの真正性を保護すること。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
11	同時セッションの制御	同時処理されるアカウントの割り当て数、又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
12	セッションのロック	定められたアイドル時間を経過した場合 又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。	Microsoftのクラウドサービスコンポーネントを利用し実施しています。
15．建物、電源(空調等)			
装置の対策			
1	構外にある装置及び情報資産のセキュリティ	構外にある情報資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、 セキュリティを適用すること。	構外にある情報端末については、2FA、暗号化、MDMによる管理、リモートワイプ等を実施し情報セキュリティを保護しています。
2	クリアデスク・クリアスクリーン方針	書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用すること。	原則、書類や取外し可能な記憶媒体は所有せず、例外として所有する場合は、ISMSの規程に従い管理を行います。
建物の情報セキュリティ対策			
3	オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用すること。	オフィスでは電子施錠設備を設け、入退室を制限しています。
4	入退室記録	重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室の手順書と記録を作成し、適切な期間保存すること。	入居するオフィス運営会社にて入退室システムを管理しています。入退室記録はオフィス運営会社にて保管しています。またセキュリティカードの割り当てについては弊社にてリストを作成し管理しています。